UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (PAC)

THE GOVERNMENT'S OPPOSITION TO THE DEFENDANT'S MOTION FOR A JUDGMENT OF ACQUITTAL PURSUANT TO FEDERAL RULE OF CRIMINAL PROCEDURE 29

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
One Saint Andrew's Plaza
New York, New York 10007

David W. Denton, Jr.
Sidhardha Kamaraju
Matthew Laroche
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S2 17 Cr. 548 (PAC)

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum of law in opposition to defendant Joshua Adam Schulte's motion for acquittal pursuant to Federal Rule of Criminal Procedure 29. After a four-week trial, a jury found Schulte guilty of making false statements to law enforcement, in violation of 18 U.S.C. § 1001, and contempt of Court, in violation of 18 U.S.C. § 401(3). The jury was unable to reach a unanimous verdict as to the remaining eight counts and, as a result, the Court granted Schulte's motion for a mistrial as to those counts. The Government intends to retry Schulte on those national security related charges, as reflected in the S3 superseding indictment, as soon as possible. As detailed below, the evidence of Schulte's guilt was more than sufficient to sustain a conviction as to all counts. Schulte's motion should be denied.[1]

[1] In light of the need to describe and discuss the trial evidence in response to Schulte's Rule 29 motion, the Government respectfully requests permission to file this brief in excess of the page limitations set forth in the Court's Individual Practices.

BACKGROUND

I. THE GOVERNMENT'S CASE

At trial, the Government presented powerful evidence that Schulte was responsible for stealing, disclosing, and attempting to disclose a massive amount of classified information. Schulte's egregious conduct began during his time with the Central Intelligence Agency ("CIA"). Furious with his management's response to Schulte's false claims concerning another employee and Schulte's loss of administrative privileges on a CIA classified computer system, Schulte responded by breaking into that computer system, stealing classified information (the "Leaked Information") about the CIA's extremely valuable cyber tool arsenal, and transmitting it to WikiLeaks, which subsequently disclosed it publicly between March and November 2017 (the "Leaks"). During multiple subsequent interviews about the Leaks with the Federal Bureau of Investigation ("FBI"), Schulte repeatedly lied about this and other conduct.

Later, after he was detained in this case, Schulte brazenly violated a protective order entered by the Court after the Court explicitly told him not to and continued to disclose and attempt to disclose classified information. From prison, Schulte used an illegal cellphone to set up encrypted email accounts and anonymous social media accounts; pretended to be another person using those accounts; deleted evidence of his activities on those accounts; threatened to breakup the United States' diplomatic relationships unless his case was dismissed; declared an "information war" against the United States; told a reporter that he was a member of the hacking group Anonymous, which had given information to WikiLeaks in the past; sent that same reporter classified national defense information about a CIA computer network and a search warrant affidavit in violation of the protective order; promised to give that reporter more sensitive information; and planned to post tweets and transmit an article with more classified national defense information about a cyber tool and CIA tradecraft.

Schulte's criminal conduct was proven through substantial evidence, including: (i) testimony of 11 CIA witnesses about, among other things, Schulte's anger at CIA management and unauthorized activities on the CIA's classified computer system DEVLAN, as well as the damage caused by the Leaks; (ii) testimony of three FBI witnesses about the investigation of Schulte's conduct at the CIA and in prison, as well as the numerous lies Schulte told to the FBI during interviews following the Leaks; (iii) testimony of four expert witnesses, including computer scientists who testified that Schulte stole the Leaked Information from DEVLAN on April 20, 2016 and that the data disseminated by WikiLeaks was the same data Schulte copied on April 20, 2016; (iv) DEVLAN computer and server log files, including from Schulte's own computer, showing that Schulte broke into DEVLAN on April 20, 2016, minutes later stole the Leaked Information, and systematically deleted and attempted to delete evidence of those activities; (v) computer log files from Schulte's home computer showing, among other things, that Schulte took steps to transmit the Leaked Information to WikiLeaks in the weeks following the theft and then reformatted his computer, thereby erasing the evidence of his activities; (vi) recordings of interviews of Schulte at the CIA during which Schulte expressed his anger at his supervisors and his desire to "punish" them for perceived slights; (vii) badge records and chat logs showing that Schulte was at his CIA computer when the Leaked Information was stolen on April 20, 2016; (viii) Schulte's prison notebooks in which he declared his "information war" and detailed his plan to disclose classified information using encrypted email and social media accounts he created in prison (the "Prison Notebooks"); (ix) testimony of a cooperating witness who explained how

Schulte used an encrypted cellphone and angrily talked about his "information war" in prison; and (x) encrypted emails sent by Schulte to a reporter containing classified information and documents subject to the protective order.

A. October 2015 Through March 2016: Schulte Becomes Angry

In the fall of 2015, Schulte began having significant problems at the CIA, which stemmed from an ongoing dispute with another CIA employee, Amol. In October 2015, Schulte and Amol each complained to their supervisor about each other, with Schulte falsely claiming that Amol made a death threat. (GX 1029; Stedman Tr. 1502-03; Weber Tr. 277-80; Sean Tr. 1633-35)).[2] In late February 2016, Amol and Schulte got into a heated argument at work. (Weber Tr. 271-73). Shortly after this dispute, on March 1, 2016, Schulte emailed the security office ("Security") and complained that Amol was abusive and had made death threats toward him. (GX 1030). Schulte also forwarded to Security his October 30 email reporting Amol's purported death threat. (*Id.*). Multiple witnesses testified that they believed Schulte's claims about Amol were false and that they had never witnessed Amol threaten others. (Stedman Tr. 1502-03; Weber Tr. 277-81; Sean Tr. 1633-35).

In the weeks that followed, Schulte grew angrier at what he perceived was his management's indifference to his claim that Amol had threatened him. (GX 1038; 1039; 1044; 1046; 1048; 1052). Eventually, Schulte filed a motion for a protective order against Amol in state court, which was initially granted. (Weber Tr. 282-84; GX 1619). As a result of the interim

[2] "GX" refers to a Government Exhibit at trial; "DX" refers to a defense exhibit at trial; and "Tr." refers to the trial transcript with the name preceding Tr. denoting which witness was testifying.

protective order, management reassigned Amol and Schulte to different branches within the Engineering Development Group ("EDG"), the group for which both worked. Schulte complained that he was being unfairly retaliated against for making a complaint against Amol, and threatened to hire a lawyer if management did not respond to his complaints. (GX 1039; 506). On March 29, 2016, Schulte submitted a form to Security, stating that he intended to meet with an attorney to pursue legal action and that the media might become involved. (GX 506). That same day, Schulte sent an email to several high-level supervisors, in which he wrote, "I just want to confirm that this punishment of removal from my current branch is for reporting to security in which my life was threatened and/or for submitting a protective order against [Amol]." (GX 1046).

Meanwhile, Schulte's state court protective order proceedings progressed, with Schulte and Amol appearing in state court on April 6, 2016. (GX 1048). Two days later, Security interviewed Schulte. (GX 508). During that interview, Schulte told Security, among other things, that he was being punished for reporting Amol's conduct; that he would "go to the media" if forced into a corner; he would "do whatever I have to do to make the situation right" and to "shed light on this"; and that his management needed to be "punished" for what they had done to him. (*Id.*).

B. Schulte Inappropriately Accessed and Altered DEVLAN

On April 4, 2016, after Schulte moved from his old branch, the Operations Support Branch ("OSB"), to a different branch in EDG, Schulte's administrative privileges to two OSB projects, OSB Libraries and Brutal Kangaroo, were revoked. (GX 1202-1; 1207-53; Leedom Tr. 976-80). Days later, on April 14, 2016, Schulte confronted a developer in OSB (Schulte's former branch), Jeremy Weber, about Schulte's loss of administrative privileges to OSB Libraries. (GX 1062; Weber Tr. 289-90). Weber told Schulte that because Schulte had been moved to a different branch, Schulte no longer required administrative privileges to OSB Libraries. (*Id.*). Schulte disagreed, and claimed that even though he had moved to another branch, he was still assigned to all of his previous projects. Weber explained that he had a different understanding but that Schulte could speak with Sean, Schulte's former supervisor, about it. (*Id.*). Schulte then spoke with Sean, but did not raise the issue of administrator privileges. (GX 1062; Sean Tr. 1651-52).

Schulte then falsely told Weber that Sean had approved the reinstatement of Schulte's administrative privileges to OSB Libraries. (GX 1062; Weber Tr. 290-91). Weber responded that he would discuss the issue with Sean, and Schulte replied that Weber should restore Schulte's privileges now because Schulte was eventually going to regain access to OSB Libraries anyway. (*Id.*). Weber and Sean then discussed the issue, and Weber emailed Schulte to inform him that, in fact, Schulte's administrative privileges to OSB Libraries would not be restored. (GX 1061). Schulte responded by again requesting that his supervisors authorize him to continue to serve as an administrator for OSB Libraries. (*Id.*).

Unbeknownst to anyone at EDG, however, on April 14, Schulte secretly used his administrative privileges to restore his access to OSB Libraries. (GX 1207-97). Weber discovered that Schulte had restored his privileges later that evening, and reported the incident to his management, who in turn raised the issue with Security. (GX 1062; Weber Tr. 528). Schulte's actions caused significant concern at the CIA because they were in direct violation of CIA policy and called into question whether Schulte could be trusted with classified information. (Weber Tr. 297-99; Leonis Tr. 577-601; GX 1062).

The CIA's concerns about Schulte were heightened by the fact that DEVLAN contained highly sensitive and classified national defense information concerning, among other things, the

CIA's cyber tool arsenal. (Weber Tr. 227; Leonis Tr. 597-601; GX 1062). The CIA protected DEVLAN by restricting outside access to it; sequestering it from the Internet; limiting access to approximately 200 individuals, each of whom possessed a Top Secret security clearance; requiring badges to enter the locked rooms secured by vault doors in which DEVLAN terminals were stored; and protecting the CIA building in which the system was housed with armed guards and perimeter fencing. (*See* Tr. 187, 194-96, 213, 552, 779, 900-01, 907).

The CIA stored much of the sensitive and highly classified information on DEVLAN within a commercially-available suite of software known as Atlassian, which included programs named Confluence (EDG's Wikipedia-like page in which users could post comments about the group's work) and Stash (the repository for, among other things, source code). (Weber Tr. 174, 215-18). Schulte was able to restore his access to OSB Libraries because he, at the time, had administrative privileges to the Atlassian services on DEVLAN. (Weber Tr. 172, 237-38). While logged in as an administrator of any of the Atlassian services, Schulte could, among other things, access and copy DEVLAN's backup files that were stored on another server (the "Backup Files"), whereas a regular user would be unable to access those Backup Files. (Leedom Tr. 950-54; Weber Tr. 252-56). Schulte, unlike regular DEVLAN users, also was very familiar with the Backup Files because he wrote the computer code that was used to create the Backup Files, was involved in making the Backup Files accessible to administrators, and managed the Backup Files including, for example, deleting old Backup Files when those files took up too much space. (Weber Tr. 223-26, 238, 252-57). As described in additional detail below, Schulte ultimately stole the Leaked Information from the Backup Files and provided them to WikiLeaks, which eventually posted it online.

C. The CIA Tried to Remove Schulte's Administrative Privileges

In response to Schulte's actions, management directed Weber and two other system administrators, David and Tim, to remove all developers,' including Schulte's, administrative privileges to the Atlassian services on DEVLAN. (Weber Tr. 300-02; David Tr. 792-804). On April 16, 2016, David and Tim began the process of taking administrative privileges away from the developers. (David Tr. 792-804). Prior to making these changes, however, David and Tim created a "snapshot" of the Confluence database (the "April 16 Snapshot"). (*Id.*; *see also* GX 1207-92; GX 1703 at 51-66). The April 16 Snapshot was a copy of the Confluence database as it existed on April 16 so that if any of the changes made to the system caused problems going forward, David and Tim could use the April 16 Snapshot to restore the system to its state on that date, and start over without doing lasting damage to the system. (*Id.*). As a result of the changes made on April 16, Schulte could no longer access the Atlassian programs directly as a system administrator and, thus, no longer had access to the Backup Files. (*Id.*).

Dave and Tim did not change the administrative password and login credentials called "SSH keys" to the OSB server that hosted the Confluence and Bamboo services. (David Tr. 804; Leedom Tr. 937). Employees could log in to the OSB server as administrators using the administrative password, which allowed them to create, delete, or revert virtual servers such as Confluence and Bamboo, and the SSH keys, which allowed them to view, edit, and delete administrative log files, such as files showing who accessed the server and when. (Leedom Tr. 945-46, 966, 989-96). Although by early April, Schulte was no longer a member of OSB and had no administrative role on the OSB server, he nevertheless secretly continued to login using the administrative password and his SSH key (the "Schulte Key"). (Leedom Tr. 989-96). As described below, Schulte used those administrative privileges on the OSB server to regain his administrative privileges to the Atlassian services, navigate to the Backup Files to steal the Leaked Information, and delete and attempt to delete evidence of his activities.

On April 18, 2016, a division supervisor within EDG, Anthony Leonis, confronted Schulte about the fact that he had improperly restored his access to OSB Libraries four days earlier. At approximately 11:00 a.m. that day, Leonis provided Schulte with a memorandum titled "Self-Granting Previously Revoked Admin Privileges on an Agency Computer Network." (Leonis Tr. 609-14; GX 1095). The memorandum described Schulte's unauthorized restoration of his administrative privileges to OSB Libraries and stated: "do not attempt to restore or provide yourself with administrative rights to any project and/or system for which they have been removed." (GX 1095). Schulte signed the memorandum, acknowledging that he understood its prohibitions. (*Id.*). Around the time Schulte received the memorandum, Schulte attempted (again) to get back his administrative privileges to OSB Libraries by falsely telling a colleague that his supervisors had authorized it. (Stedman Tr. 1508-09, 1620-21).

D. Schulte Prepared to Copy Classified Information from DEVLAN

Almost immediately after receiving and signing the memorandum, Schulte began to try to access various parts of DEVLAN as a system administrator, knowing that he was prohibited from doing so. Schulte successfully logged into the OSB server as an administrator multiple times, and knew that he still also had access through the Schulte Key. (Leedom Tr. 1014-23; GX 1203-16, 1207-26, 1209-17, 1209-20, 1209-9, 1209-3, 1209-18, 1209-19). At approximately 1:00 p.m. that same day, Schulte emailed Leonis, falsely reporting that he had "verified that all private keys with access have been destroyed/revoked" and that "[i]t seemed like overnight all my permissions within the products were removed and all my permissions on the servers themselves revoked. And all without anyone informing me." (GX 1063). At the time, Schulte sent this email, he was logged into the OSB server as an administrator and knew he still had administrative access, even though he had lied to Leonis and claimed he did not.

On April 18, Leonis also emailed staff (including Schulte) to inform the group that going forward there would only be two system administrators for the Atlassian services. (GX 1065). Later that evening, Schulte used his remaining administrative privileges on the OSB server to view log files that had been generated by the OSB server. (Leedom Tr. 1038-48; GX 1209-13, 1203-43, 1209-44, 1209-8). Schulte reviewed log files that documented (i) information about every computer command (*i.e.*, instructions to the computer) that was entered into the system, such as the date and time of the command, and (ii) all login attempts to the server. By reviewing these files, Schulte was able to see precisely what activity the system would record. (*Id.*). After Schulte viewed the log files, he locked the vault on his floor, meaning that he was the last one in the vault around the time that he was inappropriately viewing the log files. (GX 105).

E. April 20, 2016: Schulte Stole Classified Information from DEVLAN

On April 20, 2016, the EDG staff, including Schulte, was informed by email that on April 25, 2016, Confluence and Bamboo would be moved from the OSB server to a new server. (GX 1067 and 1069). This was a significant change to DEVLAN and for Schulte, who was familiar with the workings of the OSB server, and who, as described above, still secretly had administrative access to the OSB server. Once the change took effect, Schulte would no longer be able access Confluence through the OSB server using administrative privileges he retained on the server.

On April 20 at 5:30 p.m., Schulte used the administrative account on the OSB server to create a snapshot of Confluence titled "bkup." (GX 1202-17, 1209-7). A few minutes later, at 5:35 p.m., Schulte used that same account to revert Confluence to the April 16 Snapshot—*i.e.*, when Schulte still had administrative privileges to Atlassian. (GX 1202-18; Leedom Tr. 1063-65). The effect of that reversion was to restore Schulte's Atlassian administrative privileges, thus giving him the ability again to access the Backup Files. (Leedom Tr. 1073-75). While Confluence was in this reverted state, Schulte copied two specific backup files for Confluence that were created on March 3, 2016 (the "March 3 Backup Files"). (*Id.* at 953-58; GX 1207-27, 1207-30). Critically, it was virtually undisputed at trial that the March 3 Backup Files were the exact files that WikiLeaks posted online on March 7, 2016. (Leedom Tr. 1113-33; Berger Tr. 1351-66).

After a little more than an hour, Schulte then re-reverted Confluence back to its April 20, 2016 state, deleting the records of his conduct, and then deleted the "bkup" snapshot that he had created earlier that day. (GX 1202-19, 1202-21; Leedom Tr. 1064-66). To further cover his tracks, Schulte systematically deleted log files on the OSB server that recorded his conduct (such as, for example, log files that would have recorded a command to "copy" the stolen data). (Leedom Tr. 1068-99; GX 1203-1, 1203-2, 1203-66, 1203-29, 1203-64, 1203-65, 1203-61). Schulte deleted the OSB server log files by using the administrative session he had opened using the Schulte Key, which was password protected with "KingJosh3000," a password used by Schulte, and tied to the unique IP address associated with Schulte's DEVLAN computer. (Leedom Tr. 1040-1050).

The evidence introduced at trial proved conclusively that it was Schulte who, on April 20, 2016, logged into the OSB server as an administrator, reverted Confluence to its April 16, 2016 state, stole the March 3, 2016 Backup Files, and then proceeded to delete the log files of his activity while the system was in its reverted state. That evidence included, for example, log files from Schulte's computer showing that (i) Schulte created the "bkup" snapshot before reverting Confluence (GX 1202-7); (ii) Schulte reverted Confluence back to its April 16 state (GX 1202-18); (iii) Schulte reversed the reversion and took the system back to its April 20 state (GX 1202-19); (iv) Schulte deleted the "bkup" snapshot that he created (GX 1202-21); and (v) Schulte then deleted the log files on the OSB server that would have shown his conduct during the reversion (GX 1203-8, 29, 55, 56, 60, & 63). All of those files were found on Schulte's DEVLAN workstation, a fact to which the defense stipulated. (GX 3005 at 11 (agreeing that GX 1202-7, 1202-18, 1202-19, 1202-21, 1203-8, 1203-29, 1203-55, 1203-56, 1203-60, and 1203-63 were all files found on components of Schulte's DEVLAN workstation)). While Confluence reverted to its April 16 state—when Schulte had the administrative privileges necessary to access the Backup Files—the March 3 Backup Files "date accessed" time was modified, a computer action that is consistent with copying those files. (GX 1207-27 & 30). The undisputed evidence also showed that the Confluence data included in the Leaks came from those specific Backup Files. (Berger Tr. 1364-1366).

Beyond the forensic log files, documentary evidence showed that it was Schulte who entered computer commands from his DEVLAN computer to steal the Leaked Information on April 20, 2016. This included (i) an email Schulte sent to Leonis minutes after he stole the Backup Files (GX 1070); (ii) Sametime chat logs with another employee, Michael, minutes after he stole the Backup Files (GX 719); (iii) DEVLAN chat logs with Michael around the time the reversion ended when Schulte was still deleting logs of his activities (GX 1202-25); and (iv) badge records showing that Schulte locked the 8th floor vault on the evening of April 20, meaning he was the only person on the floor around the time he was stealing the Leaked Information (GX 105). Indeed, the only two times Schulte locked the 8th floor vault in 2016 were on April 18, when he was inappropriately viewing administrative log files on the OSB server after being told that he was no longer an administrator, and April 20, when he was stealing the Leaked Information. (GX 105).

F. Schulte's Cover-up and Transfer of the Leaked Information

Over the next two weeks, Schulte continued to attempt to cover up his crime and eventually transmitted the Leaked Information to WikiLeaks from his home. On the morning of April 21, 2016, just minutes after he arrived at the office, Schulte emailed Leonis to remove Schulte's access to the OSB server—the same server that he had broken into the night before to steal the Leaked Information. (GX 1071). Less than an hour later, Schulte erased the logs and contents of a USB device that had been plugged into his DEVLAN workstation the night he stole the Leaked Information. (GX 1205-1).

While Schulte was covering up his activities at the CIA, at home, he was preparing to send the Leaked Information to WikiLeaks, including by downloading programs necessary to covertly transfer the data and to securely delete evidence of his conduct. On April 23, 2016, Schulte prepared to delete a folder titled "Brutal Kangaroo," which was the name of a CIA cyber tool that Schulte developed and which was disclosed in the Leaked Information, on his home computer using a secure deletion software called Eraser Portable. (GX 1404-6). Schulte later added to the Eraser Portable queue (but did not delete) encrypted files he stored at his home. (*Id.*; Berger Tr. 1372-75, 1389-93). The next day, on April 24, Schulte ordered for same-day delivery equipment to transfer data from external hard drives (GX 1305-6; Berger Tr. 1377-78), like the hard drives that were recovered from Schulte's apartment by the FBI following the Leaks (GX 1603, 1609, and 1610; Berger Tr. 1378-79). That same day, Schulte downloaded Tails, a program that facilitates the anonymous transfer of information over the Internet and is recommended by WikiLeaks to be used in conjunction with the program TOR, which was also installed on Schulte's home computer, as a secure mechanism for transmitting sensitive information. (GX 1403-7 and 1702; Berger Tr. 1382-83).

Schulte transferred the Leaked Information overnight on April 30 into May 1, 2016. On April 30 at 11:28 a.m., Schulte downloaded Darik's Boot and Nuke, which is a program that securely deletes data so that it is impossible to recover. (GX 1402-10; Berger Tr. 1393-96). Later that night, Schulte searched on several occasions for secure wiping utilities and visited related websites, including a website titled "Kill Your Data Dead With These Tips and Tools." (GX 1305-9; Berger Tr. 1408-09). At 12:19 a.m. on May 1, 2016, Schulte mounted the D Drive, where certain encrypted files were located, onto his home computer's virtual machine to transfer the Leaked Information. (GX 1401-1). Over the next several hours through the middle of the night and early morning, Schulte repeatedly unlocked his computer to check on the status of that transfer. (GX 1401-1). Then, at approximately 3:18 a.m. on May 1, Schulte searched several times for information about "hashing" large files (a technique to confirm the integrity of transferred data) and visited related websites, including websites titled "What is the fastest way to hash md5 large files" and "how can I verify that a 1tb file transferred correctly." (*Id.*).

On May 5, 2016, after having transferred the Leaked Information, Schulte reformatted his home computer, including the D drive that contained the encrypted files. Schulte's conduct had the effect of erasing these drives. (Berger Tr. 1409).

G. Schulte's Interest in WikiLeaks and Resignation

Due to the format of the Leaked Information, it would have taken WikiLeaks a substantial amount of time to prepare it for public dissemination. (Leedom Tr. 1113-33). After a few months had passed after Schulte transmitted the Leaked Information, Schulte began to regularly search for information about WikiLeaks, which was a marked change from his prior Internet search behavior. In the six years prior to August 2016, Schulte had conducted three Google searches for WikiLeaks material and visited nine related webpages. (GX 1351). However, between August 2016 (approximately three months after he stole the Leaked Information) and January 2017, Schulte conducted at least 39 Google searches for WikiLeaks and related terms and visited 115 related webpages. (GX 1352). Schulte even conducted one search for "WikiLeaks Code," which was significant because although WikiLeaks had never published source code, the Backup Files that Schulte had transmitted to WikiLeaks contained source code, some of which was eventually disclosed in the Leaks. (GX 1, 1352; Weber Tr. 174-75; Evanchec Tr. 2272). In addition, on January 4, 2017, Schulte searched for "WikiLeaks 2017" and visited a webpage titled "WikiLeaks Vows to 'Blow You Away' in 2017 'Showdown.'" (GX 1352).

On November 10, 2016, Schulte's last day at the CIA, Schulte sent an email containing classified information to the CIA's Office of Inspector General ("OIG") that spanned several single-spaced pages. (GX 1119). In the email, Schulte claimed that he was resigning because he had expressed concerns about DEVLAN's security to his supervisors "for two full years," but that those concerns had gone unaddressed. Schulte further wrote, "This left [DEVLAN] open and easy for anyone to gain access and delete our entire EDG source code repository or even easily download and upload it in it [sic] entirety to the internet . . . . Luckily, nothing happened, but it still illustrates the lack-of-security and pure ineptitude of [one of Schulte's supervisors]." Schulte also asserted that once this "failure of leadership was discovered," the supervisor tried to "evade responsibility and blame the decentralized and insecure [sic] environment entirely on [Schulte]." (*Id.*).

Schulte's claims about raising security concerns were patently false. Schulte had never reported security concerns to his management chain and was not targeted by management because of raising purported complaints about DEVLAN's security. (Evanchec Tr. 2206; Weber Tr. 257-58; Karen Tr. 1721). Rather, the undisputed evidence was that Schulte engaged in unauthorized conduct on DEVLAN, in direct contravention of CIA policy, and that the CIA took steps to attempt to secure the system because of Schulte's brazen and illegal behavior. (GX 1062; Weber Tr. 171-73; Leonis Tr. 597-605).

H. Schulte Lied to Law Enforcement After the Leaks

On March 7, 2017, WikiLeaks posted the first of the Leaks online. The first Leak contained information from Confluence obtained from the March 3 Backup Files, which were the same files Schulte copied on April 20, 2016. (GX 1; Weber Tr. 174; Leedom 1113-33; Berger Tr. 1350-66). In several subsequent releases, the last of which occurred on or about November 17, 2017, WikiLeaks posted data about several tools from Stash, including source code. (GX 1; Weber Tr. 174-76). From the day of the initial Leak until March 14, 2017, Schulte conducted 28 searches related to the Leak and visited 91 webpages, including a search for "WikiLeaks public opinion." (GX 1353). Schulte also searched on at least six occasions for the "FBI" and visited webpages titled "FBI Prepares Hunt for the Source of CIA Documents," "WikiLeaks Reveal CIA Hacking Trove, Has Feds on Mole Hunt," and "FBI Joins CIA in Hunt for Leaker." (*Id.*).

Schulte was subsequently interviewed by the FBI on several occasions, and repeatedly lied about his conduct. For example, Schulte falsely (i) denied being responsible for the Leaks; (ii) denied having a copy of the classified email to OIG (even though the FBI recovered a copy of the email was recovered from his apartment in New York City (GX 1616)); (iii) denied taking information from DEVLAN to his home (even though he explicitly said in chats with friends that he took information from DEVLAN to his home and knew it was wrong (GX 1405-5; Evanchec Tr. 2238-39, 2242-46)); (iv) denied working on Brutal Kangaroo at his home (even though he securely deleted a folder on his home computer named Brutal Kangaroo after stealing the Leaked Information (GX 1404-6; Evanchec Tr. 2238)); and (v) denied ever making DEVLAN vulnerable to theft (even though he systematically deleted DEVLAN log files on April 20, 2016 and otherwise repeatedly misused his administrative privileges on the system (GX 1062; Weber Tr. 291-301; Leonis Tr. 576-601)). Moreover, despite being asked repeatedly about his DEVLAN activities, Schulte never mentioned anything related to his activities on April 20, 2016. (Evanchec Tr. 2178).

I. Schulte Violated the Court's Protective Order and Started An "Information War" From Prison

After being charged in this case, Schulte continued to violate the law by blatantly violating a Court entered protective order (the "Protective Order"), and continuing to disclose and attempt to disclose classified information to others from prison. In particular, the Government presented evidence that Schulte (i) emailed a reporter a copy of a search warrant affidavit, thereby violating the Protective Order, and a document containing classified national defense information about Hickok, a classified CIA computer network (the "Hickok Disclosure") (GX 812); and (ii) attempted to transmit tweets about a classified CIA cyber tool bartender (the "Bartender Tweets") (GX 809) and an article titled "Malware of the Mind" containing classified information about CIA tradecraft (the "Malware Article," together with the Hickok Disclosure and Bartender Tweets, the "MCC Leaked Information") (GX 801). Multiple CIA witnesses testified that the MCC Leaked Information contained classified and highly sensitive national defense information that they never had disclosed publicly and that doing so could have, among other things, jeopardized the safety of CIA operators in the field and the CIA's foreign intelligence gathering operations. (*See* David Tr. 786:11-24 (Hickok Disclosure); Weber Tr. 342-343: 22-2 (testifying that the Bartender Tweets "would put CIA officers' lives at risk"); Weber Tr. 337:12-17 (testifying that Weber would not disclose the CIA tradecraft that Schulte wrote in the Malware Article because doing so "would damage our potential operations"); Michael Tr. 1218-1219: 25-9 (same regarding Bartender); Stedman Tr. 1514-1515: 7-5 (disclosing Bartender publicly could jeopardize CIA operations to gather foreign intelligence).

Schulte's egregious prison conduct began around May 2018 when news articles were published about the case, including one by a reporter at the Washington Post. (Schlesinger Tr. 2467-68). As a result, the Court held a conference on May 21, 2018 at which it reiterated to Schulte the terms of the Protective Order, including that Schulte was not permitted to provide documents subject to the Protective Order to third parties, like reporters. (GX 829). The Court also explicitly instructed Schulte, "If you want to vary the terms of the protective order, your relief is not to do it on your own, Mr. Schulte, but to have your lawyer come into court and explain why there should be a modification of the order." (*Id.* at 7). Schulte confirmed he understood the Court's instructions and the terms of the Protective Order. (*Id.* at 8).

In July, Schulte's frustration grew about his case and his relatives' failure to post publicly his "articles," including the article he titled "Malware of the Mind," which he referred to as "article

10" and which contained the Malware Disclosure. (GX 801, 809). In one entry in his Prison Notebooks from July 2018, Schulte wrote, "ugh talked to my parents today & found out that my fucking articles that were uploaded to [Facebook] . . . were the wrong fucking articles." (GX 806). In an entry dated August 8, 2018, Schulte wrote that he was prepared to "breakup diplomatic relationships, close embassies, end U.S. occupation across the world" unless the Government paid him $50 billion for charging him in this case. (GX 809). This statement showed not only that Schulte was growing increasingly frustrated but also that his frustration had risen to the point that he—according to his own words—planned to destroy the United States' relationships with its allies, leading to, for example, the shuttering of U.S. embassies in other nations. Schulte was, of course, capable of releasing extremely damaging information because of the sensitive nature of his work at the CIA. (Schlesinger Tr. 2649-52; *see also* GX 809 at 11 (Schulte writing that "Vault 7 contains numerous zero-days and malware that could easily be repurposed and released onto the world in devastating fashion . . . .").

A few days after declaring that he planned to breakup the United States' diplomatic relationships, on August 13, 2018, Schulte got a contraband Samsung cellphone in prison. (GX 821, 5003). Although by that time Schulte had access to other contraband cellphones, including iPhones, he specifically wanted a Samsung cellphone because of its encryption capabilities. (Betances Tr. 2389). In a Prison Notebooks entry dated the following day, Schulte declared his "information war," noting that he "[g]ot to use [the Samsung phone] last night." (GX 809 at 3). Schulte intended to disclose classified and highly-sensitive information as part of his information war to punish the United States, which he referred to as "the most corrupt, tyrannical government on the planet." (*Id.*). Indeed, on at least two other occasions in the summer of 2018, Schulte angrily talked about his "information war" with another inmate, being careful to stop talking when he became aware that others were present. (Betances Tr. 2408-09). In the same entry of the Prison Notebooks declaring his "information war," Schulte also explicitly wrote about setting up various anonymous social media accounts and blogs that he would use in furtherance of his so-called "war," including that he planned to post links on Facebook to his "articles" and that his blog "will contain my 10 articles." (GX 809 at 3).

Just one week later, Schulte had already taken significant steps in his "information war." In a Prison Notebooks entry dated August 21, 2018, Schulte wrote about systematically deleting evidence from social media accounts and from the contraband Samsung phone. Schulte wrote, for example, "Delete all Google Docs from johnsmith," "Delete all emails from johnsmith," and "Delete all suspicious emails from my gmail." (GX 809). Schulte also wrote about setting up encrypted email accounts, which he later used to transmit classified information to the Washington Post reporter, and creating encrypted messaging accounts "all with different numbers!", including a Signal account that he later used to communicate with the Reporter. (*Id.*; *see also* GX 822).

The next day, on August 22, Schulte (pretending to be another person) used the Samsung cellphone and an encrypted email account (the "Anonymous Email Account") to send an email to the reporter asking for copies of his articles. (GX 1303-2). Schulte confirmed in his Prison Notebooks that it was, in fact, him who sent the August 22 email to the reporter, writing in an entry dated August 23, 2018, "Yesterday I started emailing [the Reporter] from the Washington Post," and Schulte also separately wrote down the password for the Anonymous Email Account in the Prison Notebooks. (GX 809; Schlesinger Tr. 2645-46). In that same August 23 entry, Schulte expressed frustration that his brother had not published his articles, writing, "[my brother] went back and forth but they decided for me not to publish the articles . . . my own fucking articles. Isnt that incredible?" (GX 809). On August 31, Schulte emailed the reporter again using the Anonymous Email Account and tried to entice the reporter to publish material on a timeframe dictated by Schulte: "If you can consent to an embargo on disclosure of the information for a limited time we would give you an exclusive to the information spanning several topics." (GX 1303-11).

Schulte's conduct continued to escalate in September and culminated with him sending classified national defense information to the Reporter. On September 1, 2018, Schulte set up the Twitter account "@FreeJasonBourne," and wrote Tweets in his Prison Notebooks that he intended to post using that account, including the Bartender Tweets and other tweets encouraging others to "send all your govts secrets here: Wikileaks." (GX 809 at 9-12). On September 2, 2018, Schulte (pretending to be another person) sent encrypted Signal messages on the Samsung phone to the reporter, in which Schulte said that he used to be a member of Anonymous, a hacking group that had provided information to WikiLeaks, and asked the reporter for help, including by "releasing" Schulte's articles. (GX 822-1; *see also* GX 1702; GX 809 at 13 (Schulte writing in an entry dated September 2, 2018, "Hopefully tonight I can setup Signal from my cell & msg [the reporter] to . . . get my fucking articles. I also need to confirm my twitter.")). In a Prison Notebooks entry dated September 12, 2018, Schulte wrote that he planned to "Schedule tweets 27th," and in another entry dated September 17, 2018, he wrote "In a week I'm going to dump all my stuff." (GX 809 at 15-16).

On September 24, 2018, Schulte began transmitting national defense information to the reporter. On that day, Schulte used the Samsung phone to send an encrypted email to the reporter via the Anonymous Email Account. Schulte attached to the email a search warrant subject to the Protective Order and his notes that contained the Hickok Disclosure. (GX 1303-34). Schulte also promised the reporter additional sensitive information regarding government officials. (*Id.*). On October 3, 2018, Schulte's "information war" was stopped before he could transmit additional national defense information, including the Malware Article and Bartender Tweets, when the FBI searched the MCC, seizing his Prison Notebooks and eventually recovering Schulte's contraband cellphone. (Schlesinger Tr. 2471, 2644).

II. THE DEFENSE CASE

Schulte called one witness, paralegal Achal Fernando-Peiris, who read an August 16, 2019 CIA memorandum into evidence (the "CIA Memorandum") (DX L). In the CIA Memorandum, an employee with the CIA's Counterintelligence Mission Center ("CIMC") sought approval to place Michael—one of Schulte's colleagues at the CIA—on administrative leave. Michael worked for a time within OSB, and he was interviewed by the CIA as part of the dispute between Amol and Schulte in 2016, as well as by the FBI on multiple occasions following the initial Leak. The CIA Memorandum, in a section titled "Justification," stated that "[Michael's] lack of cooperation with inquiries into his past activities with the primary person of interest in the FBI investigation and his unexplained activities on the computer system from which the [Vault 7 Information was stolen], raises significant concern about his truthfulness, trustworthiness, and willingness to cooperate with both routine OS reinvestigation processes and the criminal investigation into the theft from his office." (DX L at 1). The author also wrote, "CIMC believes curtailing [Michael's] access to CIA spaces and data systems is necessary to safeguard against potential future losses of sensitive and classified information." (*Id.*).

The CIA Memorandum also provided background for the administrative leave request. For example, the memorandum discussed how Michael had not been cooperative with an internal CIA investigation into Michael's physical altercation with Schulte. (DX L at 2). The CIA Memorandum also described several "concerns" with Michael, "including his close proximity to the theft of the data and his relationship with Joshua Schulte, the individual charged with the theft of the data." (*Id.* at 3). The memorandum further stated that "[f]orensic analysis of [Michael's] activity on the DEVLAN suggests that [Michael] may have additional knowledge of anomalies on the system at the time of the theft." (*Id.*). Based on these concerns, the memorandum described a "Risk Assessment" that CIMC viewed Michael's "lack of cooperation as a significant and untenable risk to the security of the operations on which he now works and any new tools he deploys for [the Center for Cyber Intelligence]." (*Id.*).

Nothing in the CIA Memorandum—whether in the "Justification" section or elsewhere—stated that the CIA viewed Michael as a potential suspect in the theft of the Leaked Information, rather than simply an employee who was uncooperative with an investigation into Schulte.

III. THE GOVERNMENT'S REBUTTAL WITNESS

The Government called Carter Hall, the Chief of CIMC's Counterespionage Department, as a rebuttal witness. (Hall Tr. 2682). Hall testified that he oversaw the drafting of the CIA Memorandum recommending that Michael be placed on administrative leave and directed that it be sent to the chief of security for approval. (*Id.* at 2683). Hall explained that the CIA did not suspect Michael as being involved in the Leaks. (*Id.* at 2684, 2692, 2694, 2737-38). Rather, he was placed on administrative leave because "[h]e had been uncooperative through the security process, both into a couple of incidents involving the defendant, as well as his own security reinvestigation processing." (*Id.* at 2683).

Hall also explained various portions of the CIA Memorandum. With respect to the part of the memorandum that stated that Michael was an employee "associated" with the Leaks investigation, Hall explained that the FBI was responsible for that investigation; Michael was not a suspect in the Leaks investigation; and Michael was associated with that investigation in that he had a close personal and professional relationship with Schulte, whom the CIA suspected of being responsible for the Leaks. (DX L at 2684-85). As to the sentence referencing Michael's "unexplained activities" on DEVLAN, Hall said that statement did not indicate the CIA's view that Michael was responsible for the theft, but rather that "[h]e had taken a screenshot on the day of the theft on the network in question" and he "was not cooperative with investigative personnel in discussing why he had done that." (*Id.* at 2685-86). Hall explained that Michael's conduct raised concerns about his trustworthiness because in order to hold a security clearance employees must be candid about their and their co-workers' activities. (*Id.* at 2686).

Hall testified multiple times that the CIA did not suspect Michael was involved in the Leaks, but rather believed Schulte was responsible. Hall's testimony was supported by the overwhelming evidence at trial, which demonstrated that it was impossible for Michael to have stolen the Leaked Information on April 20, 2016.

IV. THE VERDICT AND RULE 29 MOTION

On March 9, 2020, the jury found Schulte guilty of making false statements to law enforcement, in violation of 18 U.S.C. § 1001, and contempt of Court, in violation of 18 U.S.C.

§ 401(3). The jury was unable to reach a unanimous verdict as to the remaining eight counts and, as a result, the Court granted Schulte's motion for a mistrial as to those counts.

After the Government rested following its case-in-chief, Schulte moved pursuant to Rule 29 of the Federal Rules of Criminal Procedure for a judgment of acquittal, arguing that "even taking the evidence in the light most favorable to the government" the evidence was not "sufficient . . . to warrant a guilty verdict on the counts." (Tr. 2666). Schulte renewed that motion when the Government rested again after Hall's rebuttal testimony. (Tr. 2740). On May 15, 2020, Schulte filed a motion renewing his Rule 29 motion for acquittal as to all counts. However, the May 15 motion focused solely on the count charging Schulte with theft of Government property, in violation of 18 U.S.C. § 641.

ARGUMENT

I. THE GOVERNMENT ESTABLISHED THE ELEMENTS OF THE OFFENSES CHARGED IN INDICTMENT

Schulte's post-trial motion argues, in a footnote, that the Government presented insufficient evidence as a matter of law to convict Schulte of the counts in the Indictment. (Dkt. 397 at 1 n.1). He further argues that Count Five of the Indictment, which charged a violation of 18 U.S.C. § 641, should also be dismissed because § 641 is essentially pre-empted by 18 U.S.C. § 793. (*Id.* at 2-9). Neither argument has any merit. The Government's proof at trial was more than sufficient to support a rational conclusion that Schulte is guilty of the charged offenses. That proof demonstrated that Schulte illegally manipulated DEVLAN to give himself access that he should not have had, damaging DEVLAN in the process; used that access to steal the March 3 Backup Files and the Leaked Information about CIA cyber tools; transmitted those files to WikiLeaks knowing full well that by doing so, he would effectively destroy the value of those tools; lied about his conduct to the FBI; transmitted and attempted to transmit additional information about the CIA's cyber tools, tradecraft, and computer networks from the MCC as part of his "information war"; and violated the Court's protective order during his execution of that so-called "war." Moreover, the Court has already rejected Schulte's legal challenge to § 641. (Dkt. 284 at 10). Accordingly, Schulte's post-trial motion should be denied.

A. Applicable Law

Rule 29 provides that a "court on the defendant's motion must enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction." Fed. R. Crim. P. 29(a). A defendant challenging the sufficiency of the evidence supporting a conviction "'faces a heavy burden.'" *United States v. Glenn*, 312 F.3d 58, 63 (2d Cir. 2002) (quoting *United States v. Matthews*, 20 F.3d 538, 548 (2d Cir. 1994)); *see also United States v. Heras*, 609 F.3d 101, 105 (2d Cir. 2010). "[T]he court may enter a judgment of acquittal only if the evidence that the defendant committed the crime alleged is nonexistent or so meager that no reasonable jury could find guilt beyond a reasonable doubt." *United States v. Guadagna*, 183 F.3d 122, 130 (2d Cir. 1999) (internal quotation marks omitted).

"The Court must credit every inference that the jury might have drawn in favor of the government, and review all the evidence in conjunction, not in isolation." *United States v. Baldeo*, No. 13 Cr. 125 (PAC), 2014 WL 6807833, at *1 (S.D.N.Y. Dec. 3, 2014) (internal quotation marks and citation omitted); *see also United States v. Autuori*, 212 F.3d 105, 114 (2d Cir. 2000). A conviction must therefore be affirmed if, "'after viewing the evidence in the light most favorable to the prosecution, . . . *any* rational trier of fact could [find] the essential elements of the crime beyond a reasonable doubt.'" *United States v. Pitre*, 960 F.2d 1112, 1120 (2d Cir. 1992) (quoting

Jackson v. Virginia, 443 U.S. 307, 319 (1979)); *see also United States v. Sabhnani*, 599 F.3d 215, 241 (2d Cir. 2010); *United States v. Reifler*, 446 F.3d 65, 94-95 (2d Cir. 2006). "These standards apply whether the evidence being reviewed is direct or circumstantial." *United States v. Persico*, 645 F.3d 85, 105 (2d Cir. 2011).

B. Discussion

1. Counts One, Two, and Three: The Theft, Transmission, and Attempted Transmission of National Defense Information

Counts One, Two, and Three charge Schulte with violating 18 U.S.C. § 793(b) and (e). Those two provisions of § 793 proscribe different acts with respect to "national defense information"—§ 793(b) criminalizes unlawfully taking documents, notes, or other items connected with the national defense for the purpose of obtaining national defense information and with the intent or reason to believe that it would be used to harm the United States, while § 793(e) penalizes, among other things, the unlawful transmission of national defense information with reason to believe that the transmission could harm the United States. At trial, the Government showed that Schulte was a disgruntled CIA employee who wished to "punish" his supervisors, and who in fact did so by stealing the Leaked Information, transmitting that information to WikiLeaks, and then compounding that offense by transmitting and attempting to transmit more national defense information while detained at the MCC. Schulte's motion with respect to Counts One, Two, and Three should be denied.

First, the Leaked Information and the MCC Leaked Information contain national defense information. To qualify as national defense information, the material must relate to "the military and naval establishments and the related activities of national preparedness," *Gorin v. United States*, 312 U.S. 19, 28 (1941), and must be closely-held by the U.S. government, *United States v.*

Heine, 151 F.2d 813, 817 (2d Cir. 1945) (holding that the dissemination of information that the Government had never kept secret cannot support an Espionage Act conviction). The Leaked Information and the MCC Leaked Information meet both prongs.

Information about how a U.S. intelligence agency "carried on its work and who did what [and] information with respect to the development of an important military weapon" constitutes national defense information. *United States v. Soblen*, 301 F.2d 236, 239 (2d Cir. 1962). At trial, the Government elicited testimony from multiple CIA employees about EDG's work developing classified cyber tools to collect intelligence from foreign actors, including terrorists, and how CIA employees developed those tools using the classified computer network DEVLAN. (*See* Weber Tr. 168-170, Leonis Tr. 550-52, 556-57, David Tr. 786, Leedom Tr. 927-28, Stedman Tr. 1513-14). The Government also showed how the Leaked Information and the MCC Leaked Information pertained to the group's work and how it maintained its computer systems. For example, the Leaked Information contained user documentation for cyber tools the group developed that described, among other things, how the tool could be used and configured (GX 13, 14, 14-1, 15, 16, 16-1), and source code for other cyber tools (GX 12-2; Weber Tr. 208-09). Similarly, the MCC Leaked Information contained statements (i) describing a technique Schulte and other developers in the group used to hide data (GX 801 at 2; Weber Tr. 336-37); (ii) publicly identifying the then-secret cyber tool Bartender and associating it with the CIA (GX 809 at 10; Weber Tr. 342, Michael Tr. 1219); and (iii) describing how DEVLAN was connected to another CIA computer network through a bridge network named Hickok (GX 812 at 3; David Tr. 786-87). The Leaked Information and the MCC Leaked Information undoubtedly related to how EDG—an arm of the CIA, a U.S. intelligence agency—"carried on its work . . . with respect to the development of" sensitive cyber tools, and thus certainly constitutes national defense information. *Soblen*, 301 F.2d at 239.

Moreover, this information was closely-held by the CIA. While Schulte attempted at trial to make much of the fact that DEVLAN was operated in a collaborative manner and that, on occasion, some employees might have made mistakes with respect to access, those issues do not undermine the core fact that the CIA protected this information from public disclosure (and indeed, that it took an insider to compromise the system). First, information about EDG's work developing cyber tools was classified and was housed on a classified computer network. (*See* Weber Tr. 170, Leonis Tr. 552-57, David Tr. 786, Leedom Tr. 927-28, Stedman Tr. 1513-14). While the fact that information was classified is not dispositive, it is probative of the fact that the information was closely-held. *See United States v. Abu-Jihaad*, 630 F.3d 102, 135 (2d Cir. 2010) (finding that the fact that information was classified was relevant to determining whether the information was closely held); *see also United States v. Dedeyan*, 584 F.2d 36, 40 (4th Cir. 1978) (classification tends "to show or make more probable that the document does, in fact relate to the national defense"). Furthermore, the CIA restricted outside access to DEVLAN, sequestering it from the Internet, limiting access to about 200 CIA employees each possessing a Top Secret security clearance, requiring badges to open the vault doors to the locked rooms that housed the DEVLAN terminals, and protecting the CIA building in which the system was housed with armed guards and perimeter fencing. (*See* Weber Tr. 187, 194-96, 213, Leonis Tr. 552, David Tr. 779, 900-01, 907).

Second, with respect to Counts One and Two, the evidence also showed that it was Schulte who illegally took and transferred the Leaked Information to WikiLeaks. The evidence included, for example, Schulte's own videotaped statements and emails in which he expressed his view that, at least beginning in the spring of 2016, his management had betrayed him and needed to "punished." (*See*, *e.g.*, GX 508; GX 1046). Such motive evidence is probative of Schulte's guilt. *See Abu-Jihaad*, 630 F.3d at 139 (evidence of defendant's desire to wage jihad against the United States supported conclusion that it was the defendant who transmitted national defense information to terrorist group). The evidence further showed that as Schulte grew more frustrated, he manipulated DEVLAN to restore his administrative privileges to OSB Libraries, (GX 1061, 1062, & 1207-7), causing management to take away his and others' administrative privileges for the Atlassian services (like Confluence and Stash) (*see* Weber Tr. 302-03) and to reprimand Schulte and instruct him not to "attempt to restore or provide yourself with administrative rights to any project and/or system for which they've been removed" (GX 1095).

On April 20, just hours after learning Confluence would be moved to a new server, Schulte took a series of steps to ensure that he would retain access to Confluence in order to copy the Leaked Information. Specifically, Schulte (i) created a snapshot of the Confluence virtual machine as it existed on April 20, 2016 (GX 1202-17); (ii) blatantly disregarded the directive he had been given just two days earlier and restored his administrative privileges to Confluence, thus giving himself access to the Backup Files where the Leaked Information was stored (GX 1202-3; GX 1202-17, GX 1202-18; Leedom Tr. 1072-73, 1116-17); (iii) accessed the system in that state for more than an hour (Leedom Tr. 1065); (iv) deleted log files on the OSB server that would have shown, for example, the copying or transferring of information (*see*, *e.g.*, GX 1203-60); (v) restored Confluence back to its state before he had accessed it and stolen the Leaked Information, which deleted all of log files that would have shown, among other things, copying activity (GX 1202-19; Leedom Tr. 1065); and (vi) finally, deleted the April 20 snapshot he had created to allow him secret access to the Leaked Information, (GX 1202-21). Moreover, the evidence showed that the March 3 Backup Files which were part of the data in the Leaked Information (Berger Tr. 1351)—were "modified" on April 20, 2016, just minutes after Schulte reverted Confluence to restore his administrative access and access to the Backup Files.[3] Put simply, the Government's evidence showed that Schulte snuck into a part of DEVLAN that he had no legitimate reason for visiting, remained there for more than an hour, attempted to destroy all evidence of his activities during that period, and, that during the time Schulte was there, the very data that appeared on WikiLeaks was accessed in a manner that is consistent with copying the data. This evidence certainly gives rise to a reasonable inference for the jury to draw—and one that the Court should draw in rejecting Schulte's motion—that Schulte copied the Leaked Information on April 20, 2016. *See United States v. Sureff*, 15 F.3d 225, 229 (2d Cir. 1994) (evidence sufficient to support conviction where "there is no reasonable and innocent explanation for [Schulte's] conduct while there is a single, very plausible but criminal explanation").

Moreover, against this backdrop, the evidence also showed that it was Schulte who transmitted or caused the Leaked Information to be transmitted to WikiLeaks. Four days after he copied the Leaked Information from DEVLAN, Schulte began preparing to transmit the Leaked Information from his home, purchasing computer equipment used to transfer large quantities of data and downloading computer software that facilitated anonymous transfer activity online. (GX

[3] Although not raised in his Rule 29 motion, Schulte has repeatedly asserted that he is entitled to full mirror images of various servers, most recently making that claim in a letter to the Court dated June 8, 2020. (Dkt. 404). The Court has rejected Schulte's request on multiple occasions, and nothing that happened at trial undermines those rulings. (*See* Dkt. 329, 332).

1305-6, 1403-7). Around that same time, Schulte began experimenting with different methods to securely erase data from his home computer, including by downloading a program used to "nuke" a hard drive. (GX 1404-6; GX 1402-10). Then, between April 30 and May 1, 2016, Schulte worked late into the night on his home computer until, at approximately 3:21 am, he researched how to verify that a quantity of data of a similar size as the Backup Files he stole on April 20, 2016 had transferred correctly. (GX 1305-9). Days later, Schulte reformatted that computer, destroying all of the data on the machine. (Berger Tr. 1409).

In addition, the Government also introduced evidence that, beginning in August 2016, Schulte's interest in WikiLeaks dramatically increased, as Schulte researched WikiLeaks regularly, including searching for information about "WikiLeaks Code." (GX 1351; GX 1352). Finally, the Government showed that Schulte lied to the FBI about, among other things, the fact that he had kept a copy of his email to OIG, in which he claimed that DEVLAN was so compromised that its contents could be stolen and posted online (GX 1119), and the fact that he had taken classified information home in the past (even though Schulte admitted to doing so in a chat with a friend (*see* GX 1605-3)). Given that there is no dispute that WikiLeaks in fact received the Leaked Information, this evidence is more than sufficient to support a reasonable inference that Schulte transmitted the Leaked Information to WikiLeaks. *See Abu-Jihaad*, 630 F.3d at 135-39 (circumstantial evidence that defendant had access to the national defense information, had a motive to transmit the information, had prior contact with the recipient of the information, had previously disclosed classified information, and had sought to destroy evidence sufficient to support conviction for transmittal of national defense information).

Similarly, the evidence with respect to Count Three demonstrates that Schulte transmitted and attempted to transmit the MCC Leaked Information. First, using the Anonymous Email Account—which Schulte documented his creation and use of and recorded the password for in the Prison Notebooks (GX 809 at 5-7; Weber Tr. 339; Betances Tr. 2398-99; Schlessinger Tr. 2481-82)—Schulte transmitted information about Hickok and how it acted as a bridge between DEVLAN and another network, (GX 812 at 3), which, as described above, is national defense information, *see supra* pp. 17-18. This communication alone is sufficient to show unlawful transmission for purposes of Count Three. In addition, however, the Government also introduced evidence that showed that Schulte intended to and attempted to transmit additional national defense information, including: (i) Schulte wrote in one of his Prison Notebooks that he intended to engage in an "information war" against the United States using specific social media accounts, (GX 809 at 3); (ii) Schulte created Twitter and Wordpress accounts, (GX 809 at 5-9; GX 1304-1; GX 1301-3); (iii) Schulte drafted an "article" to include classified information about how CIA developers hid data (GX 801 at 2) and a tweet to include classified information associating a tool named Bartender with the CIA, (GX 809 at 9-16), both of which are, as described above, national defense information, *see supra* pp. 17-18; (iv) Schulte used the Samsung cellphone to access these social media and email accounts, (GX 820-402; GX 820-433; GX 820-434; GX 821; GX 3003); and (v) Schulte tried to conceal his use of these accounts, as demonstrated by his posing as his "friends and family" in communications (*see*, *e.g.*, GX 1303-6), and deletion of evidence, such as when he wrote in his Prison Notebooks to "delete suspicious emails from my gmail" (GX 809 at 5). Taken together, this evidence clearly demonstrates that Schulte intended to transmit the national defense information in the draft "article" and tweet he drafted in the Prison Notebooks. *See*, *e.g.*, *United*

States v. Desposito, 704 F.3d 221, 233 (2d Cir. 2013) ("Thus, a rational jury could find beyond a reasonable doubt that his persistent writing and mailing of letters constituted substantial steps toward obstructing his criminal trial."); *see also United States v. Steele*, 390 F. App'x. 6, 12 n. 2 (2d Cir. 2010) ("assumption of a false name, and related conduct, are admissible as evidence of consciousness of guilt, and thus of guilt itself") (internal citation omitted).

Third, the evidence showed that Schulte had the requisite *mens rea* to support a conviction under Counts One, Two, and Three. The Government introduced (i) testimony from Professor Rosenzweig about the public harms to the United States that had resulted from prior WikiLeaks disclosures, such as the recalling of the U.S. ambassador from Mexico following WikiLeaks disclosure of U.S. Department of State cables leaked by Chelsea Manning (Rosenzweig Tr. 48-49); (ii) electronic chats in which Schulte demonstrated his knowledge of Manning's leak (GX 1405-7, 1405-8), and the need for the U.S. government to protect some information from disclosure for national security reasons (GX 1405-10); (iii) Schulte's CIA security agreements in which he acknowledged that the unauthorized disclosure of classified information could "jeopardize intelligence activities" and "cause irreparable harm to the United States" (GX 405); and (iv) Schulte's emails and videotaped statements in which he described how, in the months before April 2016, he had come to feel betrayed by his management and that they needed to be "punished" (*see*, *e.g.*, GX 508; GX 1046).

Moreover, the Government also introduced Schulte's writings in his Prison Notebooks, in which he declared an "information war" against the United States government in retaliation for his prosecution and detention, expressed his desire to "break up [the United States'] diplomatic relationships" through disclosure of information he know, and encouraged disgruntled U.S.

government employees to "send all your government secrets" to WikiLeaks. (GX 809 at 2-3, 13). This evidence plainly demonstrated that Schulte copied the Leaked Information with the intention of harming the CIA, a U.S. government agency, as required for Count One, and that when he transmitted and attempted to transmit the Leaked Information and the MCC Leaked Information, he did so with reason to believe that the transmission would harm the United States, as required by Counts Two and Three, respectively.

Fourth, with respect to Counts Two and Three, the evidence demonstrated that Schulte did not have lawful possession of the Leaked Information or the MCC Leaked Information when he transmitted and attempted to transmit that information. As set forth above, Schulte transmitted the Leaked Information from his computer at his residence, transmitted the Hickok Disclosure from the MCC, and prepared the Malware Article and Bartender Tweets to transmit while at the MCC. *See supra* pp. 18-22. The Government also introduced evidence showing that classified information like the Leaked Information and the MCC Leaked Information must be maintained in secure facilities, and was not to be taken home by CIA employees. (Weber Tr. 204; Sean Tr. 1708; Bradley Tr. 1940). Accordingly, Schulte was not authorized to possess the Leaked Information at his home or the MCC Leaked Information at the MCC at the time that he transmitted and attempted to transmit it. *See*, *e.g.*, *United States v. Sterling*, 860 F.3d 233, 242 (4th Cir. 2017) (keeping classified information at defendant's home sufficient to support conviction under different provision of § 793(e) that still required defendant to have "unauthorized possession" of the information); *United States v. Hitselberger*, 991 F.Supp.2d 86, 90 (D.D.C. 2013) (same).

2. Counts Four, Five, Six, Seven, and Ten: Unauthorized Computer Access, Theft of Government Property, and Contempt of Court

The same evidence that established Schulte's guilt of the § 793 counts also demonstrates Schulte's guilt of (i) Counts Four, Six, and Seven, which charged him with unauthorized conduct on CIA computer systems, in violation of various provisions of 18 U.S.C. § 1030; (ii) Count Five, which charged him with theft of Government property, in violation of 18 U.S.C. § 641; and (iii) Count Ten, which charged him with contempt of Court, in violation of 18 U.S.C. § 403.

First, Counts Four and Six charge violations of 18 U.S.C. § 1030(a)(1) and (a)(2)(B). Both provisions require proof that the defendant knowingly accessed a computer "without authorization or exceeding authorized access" and that defendant obtained information as result. Sand et al., Modern Federal Jury Instructions ¶¶ 40A-3 & 40A-10 (2019). With respect to these elements, the defendant "exceed[ed] his authorized access" when he gave himself access to a part of DEVLAN that he was not authorized to access, *i.e.*, the Backup Files, *see United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015) ("exceed[ing] authorized access" requires that defendant trespasses into part of computer system he was not entitled to access), and obtained information when he copied the Leaked Information, *see supra* pp. 9-13. Count Four additionally requires that the obtained information was protected from unauthorized disclosure "for reasons of national defense or foreign relations," *i.e.*, the national defense information in the Leaked Information, *see supra* pp. 27-29, and that the defendant transmitted it to someone who was not authorized to receive it, *i.e.*, WikiLeaks, *see supra* pp. 13-14. *See* Sand et al., Modern Federal Jury Instructions ¶ 40A-3. With respect to Count Six, § 1030(a)(2)(B) requires that the information the defendant obtained is "from any department or agency of the United States," which the CIA indisputably is. As a result, the Government's proof at trial satisfies all of the elements of Count Four and Count Six.

Second, this same evidence demonstrates a violation of 18 U.S.C. § 641, which is charged in Count Five. Proving a § 641 violation requires that the Government show that Schulte knowingly stole "a thing of value" of the United States valued in excess of $1,000. Sand et al., Modern Federal Jury Instructions ¶ 23A-2 (2019). Intangible property can be a "thing of value" for purposes of § 641. *United States v. Girard*, 601 F.2d 69, 71 (2d Cir. 1979). Here, a CIA witness testified that the CIA invested millions of dollars into developing the types of cyber tools that Schulte provided to WikiLeaks. (Roche Tr. 1879). As a result, the evidence showing that Schulte stole the Leaked Information from the CIA on April 20 also shows that he stole a "thing of value" belonging to the U.S. government that was valued in excess of $1,000.

Schulte's renewed claim that § 641 does not criminalize the theft and disclosure of classified information is unavailing. (Dkt. 397 at 2-10). As the Court recognized in denying Schulte's motion to dismiss, the Second Circuit has squarely held that § 641 properly proscribes the disclosure of sensitive Government information where the "disclosure at issue was affirmatively prohibited by statute, regulation, policy, or longstanding agency practice." (Dkt. 284 at 10 (citing *Girard*, 601 F.2d at 71; *United States v. Jones*, 677 F. Supp. 238, 240 (S.D.N.Y. 1988) ("Given the government's long standing practice of maintaining the confidentiality of information relevant to on-going criminal investigations, and given the government's obvious interest in maintaining such confidentiality, the defendant could reasonably know the proscribed nature of his alleged actions.")); *see also United States v. Blaszczak,* 947 F.3d 19, 39 (2d Cir. 2019) ("Contrary to Defendants' strained reading of the case, we read *Girard* to hold that confidential information can itself be a 'thing of value' under Section 641.").

Schulte's argument to the contrary is premised almost entirely on a dissenting portion of Judge Winter's opinion in *United States v. Truong Dinh Hung*, 629 F.2d 908, 936 (4th Cir. 1980) which departed from the majority's conclusion that it need not reach the defendant's contentions about § 641. Not only did Judge Winter's opinion note that it was in disagreement with the Second Circuit's contrary holding in *Girard*, but the Fourth Circuit itself also later rejected Judge Winter's concerns in *United States v. McAusland*, 979 F.2d 970, 975 (4th Cir. 1992), affirming convictions under § 641 for disclosing sensitive Government contracting information.

Nor does the fact that § 793 criminalizes forms of disclosure of classified information in any way raise doubts about the sufficiency of the Government's evidence of Schulte's guilt under § 641. Schulte cites no law whatsoever for the proposition that the existence of a specific statutory scheme regulating the conduct at issue precludes the application of a more general statute that, by its terms, also applies. Indeed, it is not uncommon for criminal conduct to be punishable under multiple statutes of varying specificity, and the overlap in statutory schemes does not preclude application of a more general statute. For example, the Second Circuit has routinely upheld prosecutions for defrauding U.S. Government agencies in violation of 18 U.S.C. § 371 even when a more specific statute also proscribes the particular conduct at issue. *See, e.g.*, *United States v. Bilzerian*, 926 F.2d 1285 (2d Cir. 1991) (rejecting as "unpersuasive" claim that "Bilzerian would have us rule that when conduct is chargeable under the specific offense clause, the government is precluded from prosecuting under the defraud clause"); *United States v. Gurary*, 860 F.2d 521, 525 (2d Cir. 1988) (prosecution for defrauding the Internal Revenue Service (the "IRS") by supplying false information that would be used on tax returns); *United States v. Nersesian*, 824 F.2d 1294, 1309 (2d Cir. 1987) (prosecution for defrauding the IRS where defendant agreed to engage in structured transactions designed to evade bank currency transaction reporting requirements).

Instead, Schulte falls back on the purported need to construe the statute to avoid what he asserts would be constitutional infirmities. But the Court in this case has already rejected Schulte's claim that the application of § 641 raises constitutional concerns, consistent with the Second Circuit's binding precedent on point. (Dkt. 284 at 10).

Third, Count Seven charges a violation of § 1030(a)(5)(A), which criminalizes the intentional transmission of, among other things, any "code or command" that causes "damage" without authorization to a "protected computer." The statute defines a "protected computer" to include, among other things, "a computer exclusively for the use of . . . the United States" and "damage" to include, among other things, "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(2)(A) & (e)(8). In this case, a rational jury could find that Schulte violated the statute both when he transmitted commands over DEVLAN to restore the Confluence virtual machine back to the April 20 snapshot, thus destroying the Confluence virtual machine log files, and his transmission of other commands over DEVLAN to delete log files from the OSB server, which in both instances rendered those log files, *i.e.*, "data" or "information," unavailable.

Fourth, Count Ten charges Schulte with contempt of Court, in violation of 18 U.S.C. § 401(3), which requires proof that "(1) the court entered a reasonably specific order; (2) defendant knew of that order; (3) defendant violated that order; and (4) his violation was willful." *United States v. Cutler*, 58 F.3d 825, 834 (2d Cir. 1995). In this case, the Protective Order Schulte is charged with violating is perfectly clear that materials designated under it "may be disclosed only by defense counsel" (*i.e.*, not Schulte) to a delineated list of individuals which did not include reporters (GX 828 at 1-2); Schulte specifically acknowledged his understanding of this restriction to the Court at the May 21, 2018 conference (GX 829 at 7); and nevertheless, on September 24, 2018, Schulte emailed a copy of a search warrant affidavit prominently stamped as subject to the Protective Order to the reporter with *The Washington Post* in an attempt to convince that reporter to write an article about this case (GX 812). The evidence underlying Count Ten is more than sufficient to support Schulte's conviction for criminal contempt.

3. Counts Eight and Nine: False Statements and Obstruction of Justice

Finally, the Court should reject Schulte's challenge to Counts Eight and Nine. Count Eight charges Schulte with making material false statements to the FBI and the U.S. Attorney's Office in violation of 18 U.S.C. § 1001 and Count Nine charges Schulte with obstructing the investigation into the Leaked Information.

Count Eight requires proof that Schulte knowingly made material misrepresentations to U.S. law enforcement agency about a matter within that agency's jurisdiction. *See United States v. Coplan*, 703 F.3d 46, 78 (2d Cir. 2012). A false statement is material under § 1001 if it (i) had "a natural tendency to influence, or [is] capable of influencing, the decision of the decisionmaking body to which it was addressed," *United States v. Gaudin*, 515 U.S. 506, 609 (1995), or (ii) was "capable of distracting government investigators' attention away from" a critical matter, *United States v. Stewart*, 433 F.3d 273, 318 (2d Cir. 2006). In this case, Schulte made several material misrepresentations to the FBI and the U.S. Attorney's Office (which indisputably are responsible for conducting criminal investigations). For example, Schulte stated that he had never intentionally made DEVLAN more vulnerable to attack (Evanchec Tr. 2235) even though he manipulated the system on April 20, 2016 so that he could attack it, *see supra* pp. 9-13. Obviously, network activity on April 20, 2016 was critically important to the Government's investigation, given that that was the day on which the March 3 Backup Files—the contents of which WikiLeaks disclosed—were last accessed. Moreover, Schulte claimed to the FBI that he had not kept a copy of his email to OIG, which contained classified information (GX 1616; Leonis Tr. 642-43), but the FBI discovered a copy of the email at Schulte's apartment in New York (Evanchec Tr. 2179). A rational jury could certainly conclude that this misstatement was intentional, given that Schulte had kept several emails from the CIA about this dispute with CIA management at his apartment (GX 1117; Evanchec Tr. 2253), which supports that Schulte deliberately selected and retained CIA emails related to that dispute. A rational jury could also conclude that the fact that Schulte kept the OIG email and others was material, in light of testimony from an FBI agent that Schulte's emails about his dispute with management showed a "motivation to do something in retaliation to the CIA" (Evanchec Tr. 2205), a conclusion that is bolstered by the fact that Schulte had kept such emails for months after leaving the CIA. Schulte also informed the FBI that he had never worked on Brutal Kangaroo at home, even though he used a secure eraser program to delete a folder from his computer named Brutal Kangaroo just days after stealing the Leaked Information. (Berger Tr. 1432; Evanchec Tr. 2238; GX 1404-6). Similarly, Schulte told the FBI that he did not take any classified information from DEVLAN home, even though he admitted to doing so in an electronic chat with one of his friends (GX 1605-3). Obviously, the fact that Schulte had data for Brutal Kangaroo, one of the tools revealed by WikiLeaks, and other classified material on his home computer would be material, given that such conduct could itself constitute the criminal unauthorized retention of national defense information under 18 U.S.C. § 793(e), *see*, *e.g.*, *Sterling*, 860 F.3d at 242 (retention of national defense information at defendant's home violated § 793(e)), and was "capable of distracting government investigators' attention away from" a critical matter, *see Stewart*, 433 F.3d at 318, namely further forensic inquiry of Schulte's home computer, *see supra* pp. 13-14. In short, the evidence at trial was more than sufficient to support Schulte's conviction on Count Eight.

This same conduct also demonstrates Schulte's guilt of obstruction of justice, as charged in Count Nine. That count requires proof that there was a pending judicial proceeding, like a grand jury proceeding, that Schulte knew about that proceeding, and that Schulte corruptly sought to impede that proceeding. Sand et al., Modern Federal Jury Instructions ¶ 46-3 (2019). The evidence shows that during the FBI's initial interview of Schulte, an FBI agent delivered two grand jury subpoenas to Schulte, one calling for his testimony, and the other calling for production of Schulte's cellphone, (Evanchec Tr. 2218), demonstrating the first two elements. A rational jury could clearly infer that Schulte wanted to obstruct that grand jury proceeding because he knew that the grand jury sought his testimony and evidence from his electronic devices, but nevertheless sought to deter the FBI from further investigating, for example, Schulte or Schulte's home media and presenting that information to the grand jury (which, as described above, contains incriminating evidence, such as Schulte's reformatting of his home computer shortly after stealing and transferring the Leaked Information, *see supra* pp. 13-14).

CONCLUSION

For the foregoing reasons, the Government respectfully submits that the Court should deny Schulte's Rule 29 motion.

Dated: New York, New York
June 19, 2020

Respectfully Submitted,

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York

By: /s/
David W. Denton, Jr.
Sidhardha Kamaraju
Matthew Laroche
Assistant United States Attorneys
212-637-2744/6523/2420

Cc: Defense Counsel
(Via ECF)